



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ : H04L 9/32, G06F 12/14, 1/00	A1	(11) Numéro de publication internationale: WO 99/31845 (43) Date de publication internationale: 24 juin 1999 (24.06.99)
(21) Numéro de la demande internationale: PCT/FR98/02753 (22) Date de dépôt international: 16 décembre 1998 (16.12.98) (30) Données relatives à la priorité: 97/15971 16 décembre 1997 (16.12.97) FR (71) Déposant (pour tous les Etats désignés sauf US): SCHLUMBERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F-92120 Montrouge (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): BRAHAMI, Lionel [FR/FR]; 26, place Jules Ferry, F-92120 Montrouge (FR). RIGAL, Vincent [FR/FR]; 40, avenue de la Gare, F-92330 Sceaux (FR). (74) Mandataire: MACQUET, Christophe; Schlumberger Systèmes, Transactions Electroniques, Boîte postale 620-04, F-92542 Montrouge Cedex (FR).		(81) Etats désignés: CN, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée <i>Avec rapport de recherche internationale.</i> <i>Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont requies.</i>
(54) Title: METHOD FOR MAKING SECURE THE TRANSMISSION OF A MESSAGE FROM A TRANSMITTING DEVICE TO A RECEIVING DEVICE (54) Titre: PROCEDE DE SECURISATION DE LA TRANSMISSION D'UN MESSAGE D'UN DISPOSITIF EMETTEUR A UN DISPOSITIF RECEPTEUR (57) Abstract <p>The invention concerns a method for making secure the transmission of a message (Prgm) from a transmitting device (E) to a receiving device (R), characterised in that: the message (Prgm) is split into n elementary units (I), n being a number not less than 1; a logical property (P) is defined such that, for each elementary unit (I), the logical property (P), applied to an authentic elementary unit (I), gives a true logical value; the message (Prgm) is encrypted by the transmitting device (E) encryption means using an encryption algorithm comprising a key (Kc) so as to obtain a result Kc(Prgm); The encrypted result Kc(Prgm) is transmitted by the transmitting device (E) to the receiving device (R); the encrypted result Kc(Prgm) is decrypted by the receiving device (R) using a decryption algorithm comprising a secret key (Kd) so as to obtain a decrypted result Kd(Kc(Prgm)); the decrypted result Kd(Kc(Prgm)) is split into elementary units (I); the logical property (P) is applied to the elementary units (I) so as to obtain, for each unit, a true logical value or a false logical value. The method is particularly applicable to smart cards.</p> (57) Abrégé <p>L'invention concerne un procédé de sécurisation de la transmission d'un message (Prgm) d'un dispositif émetteur (E) à un dispositif récepteur (R). Le procédé de l'invention se caractérise en ce que: le message (Prgm) est divisé en n unités élémentaires (I), n étant un nombre supérieur ou égal à 1; une propriété logique (P) est définie de manière que, pour toute unité élémentaire (I), la propriété logique (P), appliquée à une unité élémentaire (I) authentique, donne une valeur logique du type vrai; le message (Prgm) est crypté par des moyens de cryptage du dispositif émetteur (E) à l'aide d'un algorithme de cryptage comportant une clé (Kc) de manière à obtenir un résultat Kc(Prgm); le résultat crypté Kc(Prgm) est transmis par le dispositif émetteur (E) au dispositif récepteur (R); le résultat crypté Kc(Prgm) est décrypté par le dispositif récepteur (R) à l'aide d'un algorithme de décryptage comportant une clé secrète (Kd) de manière à obtenir un résultat décrypté Kd(Kc(Prgm)); le résultat décrypté Kd(Kc(Prgm)) est divisé en unités élémentaires (I); la propriété logique (P) est appliquée aux unités élémentaires (I) de manière à obtenir, pour chaque unité, une valeur logique du type vrai ou du type faux. La mise en oeuvre de l'invention s'effectue notamment dans le domaine des cartes à puce.</p>		

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

**PROCEDE DE SECURISATION DE LA TRANSMISSION D'UN
MESSAGE D'UN DISPOSITIF EMETTEUR A UN DISPOSITIF
RECEPTEUR**

L'invention concerne un procédé de sécurisation de la
5 transmission de messages d'un dispositif émetteur à un dispositif
récepteur.

Lorsqu'une information est transmise d'un dispositif
émetteur à un dispositif récepteur, cette information, contenue dans
un message, est susceptible d'être altérée au cours de sa
10 transmission. Cette altération peut provenir soit, d'un défaut dans
l'émission, la transmission ou la réception du message soit, d'une
fraude d'un tiers. Le message reçu n'est alors pas intègre.

C'est la raison pour laquelle on a développé des procédés qui
permettent de vérifier l'intégrité des messages transmis.

15 Par ailleurs, lorsqu'une information est transmise d'un
dispositif émetteur à un dispositif récepteur, il est parfois utile de
rendre le message confidentiel de manière à réserver l'accès de ladite
information à un nombre limité de personnes, en général l'émetteur et
le récepteur du message.

20 C'est la raison pour laquelle on a développé des procédés
permettant de préserver la confidentialité d'un message.

Enfin, lorsqu'une information contenue dans un message
est transmise à un dispositif récepteur, il est bien souvent utile
d'authentifier ce message comme provenant effectivement du
25 dispositif émetteur.

C'est la raison pour laquelle on a développé des procédés
d'authentification des messages.

Les procédés connus de vérification de l'intégrité, de préservation de la confidentialité et d'authentification, c'est-à-dire de sécurisation des messages, consistent généralement à crypter le message et à lui joindre un certificat avant sa transmission. Le
5 dispositif récepteur décrypte alors le message, vérifie le certificat et, éventuellement, dans le cas où ledit message est un programme informatique, l'exécute.

Ces procédés présentent une évidente lourdeur, dans la mesure où le décryptage et la vérification du certificat imposent
10 chacune une opération. C'est le cas, en particulier, lorsque les opérations de cryptage et de décryptage sont longues.

Considérant ce qui précède, un problème que se propose de résoudre l'invention est de réaliser un procédé de sécurisation de la transmission d'un message d'un dispositif émetteur à un dispositif
15 récepteur qui ne nécessite pas la mise en oeuvre des deux étapes précitées de décryptage du message et de vérification du certificat.

Eu égard au problème posé ci-dessus l'invention a pour objet un procédé de sécurisation de la transmission d'un message d'un dispositif émetteur à un dispositif récepteur, caractérisé en ce
20 que :

- le message est divisé en n unités élémentaires, n étant un nombre supérieur ou égal à 1 ;

- une propriété logique est définie de manière que, pour toute unité élémentaire, la propriété logique, appliquée à une unité
25 élémentaire authentique, donne une valeur logique du type vrai ;

- le message est crypté par des moyens de cryptage du dispositif émetteur à l'aide d'un algorithme de cryptage comportant

une clé de manière à obtenir un résultat crypté ;

- le résultat crypté est transmis par le dispositif émetteur au dispositif récepteur ;

- le résultat crypté est décrypté par le dispositif récepteur à l'aide d'un algorithme de décryptage comportant une clé secrète de manière à obtenir un résultat décrypté ;

- le résultat décrypté est divisé en unités élémentaires ;
- la propriété logique est appliquée aux unités élémentaires de manière à obtenir, pour chaque unité, une valeur logique du type vrai ou du type faux.

- le message est considéré comme authentique et intègre si, pour chaque unité, les valeurs logiques ont une valeur du type vrai.

Le message est alors avantageusement stocké.

On notera par ailleurs que, de manière avantageuse, le message Prgm est un programme informatique susceptible d'être exécuté et/ou d'être interprété par le dispositif récepteur R. Les unités élémentaires sont des instructions du programme Prgm. La propriété P, appliquée à une unité élémentaire I, donne une valeur logique de type vrai lorsque l'unité élémentaire I est exécutable et/ou interprétable. La propriété P, appliquée à une unité élémentaire I, donne une valeur logique de type faux lorsque l'unité élémentaire I n'est pas exécutable et/ou interprétable. Le dispositif récepteur R est un objet portable à mémoire du type carte à puce. Le dispositif récepteur R comporte un objet portable à mémoire du type carte à puce. L'objet portable à mémoire est un module d'identification abonné (SIM). Le message Prgm est écrit dans un langage interprété

de haut niveau. Le langage de haut niveau est le langage Java. Le programme informatique est formé d'un ensemble d'instructions précompilées. Le message Prgm est crypté en flux continu ou en blocs chaînés. Le message Prgm est crypté en blocs et en ce que les blocs
5 du message Prgm crypté sont permutés. Un des blocs permutés est un bloc de début ou de fin du message Prgm. Le résultat $Kc(Prgm)$ est décrypté par blocs, chaque bloc crypté étant à l'origine d'un bloc décrypté prenant la place du bloc crypté. Les algorithmes de cryptage et de décryptage font intervenir un aléa, transmis par le dispositif
10 émetteur E, au dispositif récepteur R. Le message Prgm est enregistré, après vérification, dans une mémoire non volatile du dispositif récepteur R.

Cette invention sera mieux comprise à la lecture de la description non limitative qui va suivre.

15 Selon l'invention, le message Prgm est transmis d'un dispositif émetteur E à un dispositif récepteur R.

Le message Prgm est par exemple un programme informatique susceptible d'être exécuté et/ou interprété.

Le dispositif émetteur E est, par exemple, un serveur, un
20 ordinateur, une station émettrice dans un réseau de télécommunication ou un lecteur de cartes à puce avec ou sans contact, bref, tout dispositif capable de crypter et d'émettre un message. Bien entendu, le dispositif émetteur E doit être considéré dans un sens large comme incluant des dispositifs complexes formés
25 notamment de parties physiquement séparées, une partie assurant par exemple le cryptage du message, une autre, l'émission stricto sensu dudit message.

Le dispositif récepteur R est, par exemple, un ordinateur éventuellement muni d'un lecteur de carte à puce et d'une carte insérée dans ledit lecteur, une station réceptrice dans un réseau de télécommunication, un téléphone portable muni ou non d'un module d'identification abonné (SIM) voire même une carte à puce ou un tel module, bref, tout dispositif capable de recevoir un message voire de stocker ce message et, avantageusement, lorsque le message est un programme informatique, d'interpréter et/ou d'exécuter ce programme. Dans le cas où le dispositif récepteur comporte
10 avantageusement un objet portable à mémoire du type carte à puce, cet objet portable peut être une carte de paiement ou une carte de contrôle d'accès, par exemple, à un réseau informatique.

Dans la suite de l'exposé de l'invention, on se limitera aux exemples où le message est un programme informatique Prgm.

15 Selon l'invention, ce programme informatique Prgm est divisé en n unités élémentaires I, n étant un nombre entier supérieur ou égal à 1. Il s'agit d'instructions, de blocs d'instructions ou, dans le cas où le programme Prgm est rédigé dans un langage interprétable du type Java, d'instructions précompilées du programme (ou
20 bytecodes).

Selon l'invention, une propriété logique P est définie de manière que, pour toute unité élémentaire I, cette propriété P, appliquée à une unité élémentaire authentique, donne une valeur logique P(I) du type vrai. On cherchera néanmoins à trouver une
25 propriété P qui, appliquée à une unité élémentaire I, donne une valeur logique P(I) du type faux lorsque ladite unité élémentaire I a été modifiée et correspond par exemple à une instruction non

reconnaissable du programme, notamment non susceptible d'être interprétable et/ou exécutable.

Selon l'invention, le programme Prgm est crypté par des moyens de cryptage du dispositif émetteur E à l'aide d'un algorithme de cryptage comportant une clé Kc connue dudit dispositif E de manière à obtenir un résultat Kc(Prgm). Le cryptage garantit la confidentialité du programme Prgm lors de son émission et de sa réception, mais, surtout, durant sa transmission au dispositif récepteur R. Ce résultat Kc(Prgm) est alors transmis par le dispositif E, au dispositif récepteur R.

Il est ensuite décrypté par ce dispositif R à l'aide d'un algorithme de cryptage comportant une clé secrète Kd, connue du dispositif récepteur. Un résultat décrypté Kd(Kc(Prgm)) est alors obtenu.

Cette clé Kc peut être propre au dispositif E et connue du dispositif R, ou propre au dispositif R et par ailleurs connue du dispositif E. Un exemple de la première configuration est le cas où le dispositif R est abonné à un service délivré par le dispositif émetteur. Un exemple de la seconde configuration est le cas où le dispositif récepteur, lors de sa requête d'une transmission du programme, fournit la clé Kc, la clé Kd de décryptage restant connue du seul dispositif récepteur. Un autre exemple de la même configuration est le cas où Kc et Kd sont identiques (système à clé privée), et où cette clé est envoyée, sous forme cryptée, par le dispositif récepteur, au dispositif émetteur.

Selon l'invention, le résultat décrypté Kd(Kc(Prgm)) est divisé ou décomposé en n unités élémentaires, images des ou correspondant

aux n unités élémentaires résultant de la division du programme Prgm dans le dispositif émetteur E.

La propriété logique P est alors appliquée auxdites n unités élémentaires de manière à obtenir, pour chaque unité, une valeur
5 logique du type vrai ou du type faux.

Dans le cas où toutes les valeurs logiques sont du type vrai, on a une forte probabilité que le programme décrypté soit identique au programme crypté et que la clé ayant servi au cryptage soit la clé Kc attendue. Le dispositif récepteur R en déduit alors que le
10 programme Prgm est intègre et qu'il a été émis par un dispositif émetteur E disposant de la clef Kc, donc authentique.

Par contre, dans le cas où une valeur logique au moins est du type faux, le programme décrypté est différent de Prgm et le dispositif récepteur R en déduit que le programme Prgm a fait l'objet
15 d'au moins une modification à l'émission, à la réception ou durant sa transmission et/ou que ledit programme Prgm a crypté le message avec une clé autre que Kc, une clé non attendue. Le programme est n'est alors pas intègre ou pas authentique.

L'invention permet donc de garantir, en une seule opération
20 de cryptage-décryptage, à la fois l'intégrité, l'authentification et la confidentialité du programme Prgm.

Si l'on considère par exemple que les instructions du langage informatique dans lequel est rédigé le programme Prgm sont des instructions codées sur quatre octets, il y a, en théorie, 2^{32} codes
25 possibles pour définir une instruction. Bien entendu, certains codes, définis par un ensemble de paramètres, ne correspondent à aucune instruction compréhensible. De plus, certains paramètres de certains

codes, typiquement les trois derniers octets, n'ont que certaines valeurs autorisées. Une adresse mémoire ne peut ainsi être négative, ou se situer en dehors de l'espace alloué au programme Prgm. C'est la raison pour laquelle la propriété P comporte un avantageusement un test de paramètres, ledit test dépendant du type d'instruction.

Si l'on définit le taux de non-détection unitaire C comme étant le pourcentage des instructions possibles qui ne sont pas reconnues comme fausses par l'application de la propriété P lors du décryptage et suite à une modification ponctuelle du programme Prgm, la probabilité que le dispositif récepteur R ne détecte pas la fraude est, lorsque la modification ponctuelle est à l'origine d'une modification sur chaque instruction du résultat décrypté :

$$\text{prob} = (1 - C)^n.$$

Pour les valeurs typiques suivantes, on obtient les probabilités prob suivantes :

n	C (%)	prob
256	10%	1.9E-12
128	10%	1.4E-06
512	5%	3.9E-12
128	5%	1.4E-03

On constate que la probabilité qu'une modification notamment frauduleuse passe inaperçue est très faible, sauf dans les cas de programmes comportant peu d'instructions et dont le taux de non-détection unitaire C est très élevé. Cette probabilité est a fortiori très faible dans le cas où le programme a été crypté par une clé autre que Kc.

Comparée aux opérations de cryptage usuelles, l'application de la propriété P ne nécessite pas une mise en oeuvre trop lourde

notamment un temps de calcul trop long. Elle permet la détection des erreurs dans tous les types de programmes Prgm dès lors que l'algorithme de cryptage est de bonne qualité, eu égard au caractère pseudo-aléatoire de tout décryptage d'une suite d'instructions
5 falsifiées.

L'algorithme de cryptage est avantageusement du type en blocs chaînés ou en flux continu. Ainsi, une modification d'une instruction élémentaire entraînera une modification d'autres instructions. Par contre, lorsque l'algorithme procède uniquement par
10 blocs, le programme crypté peut être décomposé en une suite de par exemple n blocs correspondant peu ou prou aux n unités élémentaires. En modifiant un bloc et en observant le comportement du dispositif récepteur, la probabilité prob que la modification ne soit pas détectée est alors est égale à $1 - C$, donc très élevée.

15 De manière à éviter une modification dirigée sur le bloc de tête ou de queue du programme crypté, on permute, par exemple, les blocs du programme crypté, de manière que lesdits blocs de tête et de queue du programme soient à un endroit qui ne soit pas prédictible par un fraudeur, mais néanmoins connu des dispositifs E et R.

20 La confidentialité est par ailleurs améliorée lorsque l'algorithme de cryptage fait intervenir un aléa généré par exemple par le dispositif récepteur R et communiqué au dispositif émetteur E. Il peut s'agir, par exemple, d'une opération "ou exclusif" appliquée sur un nombre d'octets déterminé du programme ou sur sa totalité avant
25 cryptage.

On pourra enfin introduire en début et/ou en fin de programme, avant cryptage, des instructions vides (NOP), que le

dispositif récepteur reconnaîtra en appliquant la propriété P, puis éliminera.

Dans un premier mode de mise en oeuvre de l'invention, le dispositif émetteur E est une station de base d'un réseau de
5 télécommunication GSM (Global System for Mobil communication) ou de tout autre système de téléphonie mobile faisant intervenir un module de sécurité, le dispositif récepteur R est un module d'identification abonné SIM associé à un téléphone mobile. Le programme Prgm, destiné à être téléchargé dans ledit module SIM, est
10 codé sous la forme d'instructions précompilées (bytecodes) rédigées par exemple dans le langage Java.

Bien entendu, l'invention s'applique de la même manière aux d'autres systèmes à cartes à puces, tels que des systèmes de paiement ou de contrôle d'accès.

15 Dans ce premier mode de mise en oeuvre de l'invention, le programme est divisé en n unités élémentaires, une unité élémentaire étant une instruction précompilée d'un nombre de bits déterminé (fixe ou dépendant du type d'instruction).

La propriété logique P est définie de manière qu'elle prenne
20 une valeur logique vrai lorsque l'unité élémentaire à laquelle elle est appliquée est une instruction exécutable (ou interprétable) ou correspond à une instruction NOP.

Le programme Prgm est alors crypté par le dispositif émetteur E avec un algorithme de cryptage, par exemple du type RSA
25 (Rivest, Shamir et Adelman) tel que décrit dans le brevet US-4,405,829. Un résultat de cryptage $Kc(Prgm)$, fonction de la clé Kc, est alors obtenu.

Ce résultat $Kc(Prgm)$, en définitive le programme crypté, est transmis par la station de base à une station émettrice qui lui est associée puis à des moyens de réception du téléphone mobile. Il est alors chargé dans la carte où il est enregistré dans une mémoire non volatile EEPROM avant l'opération de décryptage, compte tenu de la
5 lenteur de cette opération mise en oeuvre sur un module SIM.

Le résultat $Kc(Prgm)$ est ensuite décrypté à l'aide d'un algorithme de décryptage comportant une clé secrète Kd . Chaque bloc du résultat décrypté est enregistré dans la mémoire non volatile
10 EEPROM du module SIM, à l'adresse du bloc du résultat crypté correspondant. Ainsi, l'espace mémoire utilisé pour la mise en oeuvre du décryptage selon l'invention est minimal. On notera que, dans une variante de mise en oeuvre de l'invention, à l'aide d'au moins un espace mémoire libre correspondant à un bloc, on peut enregistrer les
15 blocs du résultat décrypté à des adresses mémoire différentes des blocs cryptés auxquels ils correspondent. Une permutation circulaire est tout aussi possible, améliorant la sécurisation du programme durant l'étape de décryptage.

L'application de la propriété P s'effectue de préférence à la
20 fin du décryptage complet du résultat crypté $Kc(Prgm)$, le résultat final (programme accepté ou refusé) n'étant donné qu'à la fin de toutes les vérifications. Ainsi, le fraudeur ne peut pas détecter simplement l'unité élémentaire I reconnue comme donnant une valeur logique fausse lors de l'application de la propriété P .

25 Compte tenu de la faible mémoire disponible dans le module SIM, une fonction de calcul simple de la propriété P est mise en oeuvre. Il s'agit d'une fonction mise en oeuvre par l'interpréteur lui-

même. Une fois que le résultat crypté est décrypté, l'interpréteur interprète le résultat décrypté en regardant si les instructions ont un sens ou non. En définitive, l'interpréteur effectue l'analyse du programme comme il le ferait lors d'une interprétation normale, sans
5 toutefois que ladite interprétation soit suivie d'effet autre que la vérification que le résultat décrypté correspond bien à un programme Prgm.

Dans un second mode de mise en oeuvre de l'invention, le dispositif émetteur E est un serveur comportant une forme
10 précompilée et cryptée $Kc(Prgm)$ d'un programme Prgm, rédigé par exemple dans le langage Java. Le dispositif récepteur R est un ordinateur personnel, qui sera utilement muni d'un lecteur de carte à puce dans lequel est insérée une carte. L'ordinateur personnel comporte un disque dur et une zone mémoire sûre, c'est-à-dire qui
15 n'est pas susceptible d'être lue ou écrite par un tiers, pour le stockage, temporaire ou définitif, des résultats décryptés $Kd(Kc(Prgm))$ et des clés. L'ordinateur comprend par ailleurs un logiciel de chargement des programmes Prgm appelé Loader invoqué chaque fois qu'il est nécessaire de charger un programme Prgm précompilé, avant
20 que ledit programme Prgm soit utilisé (interprété ou exécuté). Dans le présent second mode de mise en oeuvre de l'invention, ce logiciel inclut une fonction de décryptage, qui comporte avantageusement des éléments fonctionnels nécessaires au décryptage et notamment des éléments de l'algorithme de décryptage. Le logiciel de chargement des
25 programmes est alors dit surchargé. Bien entendu, d'autres éléments fonctionnels nécessaires au décryptage peuvent être contenus dans une mémoire non volatile de la carte à puce. Ces éléments seront

alors appelés par le logiciel de chargement des programmes et la fonction de décryptage. Ainsi, le logiciel de chargement permet, en association avec la carte, le décryptage du résultat $Kc(Prgm)$ et la vérification du résultat décrypté $Kd(Kc(Prgm))$ avant l'interprétation
5 dudit résultat décrypté $Kd(Kc(Prgm))$, c'est-à-dire, lorsque la propriété P a été appliquée avec succès, le programme $Prgm$, et l'exécution de ce programme $Prgm$.

Les contraintes de temps et d'espace mémoire qui ont été évoquées lors de la description du premier mode de mise en oeuvre du
10 procédé de l'invention sont, dans ce second mode de mise en oeuvre, moindres, étant donné que la carte est ici uniquement utilisée comme un support physique sécurisé d'une ou plusieurs clés ou éléments, des tables par exemple, nécessaires au décryptage. La carte peut même contenir la totalité de l'algorithme secret de décryptage.

15 La propriété P peut, de ce fait, être non seulement du type de celle précitée, ou alors, être une propriété particulière dont on implémentera l'algorithme de vérification. L'algorithme de vérification vérifie dans un exemple les instructions précompilées à chaque fois qu'un bloc instruction(s) du résultat crypté est décrypté.

20 Les phases d'échange entre, d'une part, l'ordinateur personnel muni de l'interpréteur, du dispositif de chargement et associé à un lecteur de carte dans lequel est insérée la carte et, d'autre part, la carte, peuvent se décomposer en trois phases : une phase d'initialisation, une phase de transfert et une phase de
25 décryptage/vérification.

La phase d'initialisation est en fait une phase d'échange d'un couple de clés publique et secrète. Cette phase est lancée lors de

l'initialisation du processus de décryptage. Les couples de clés ne sont pas écrits sur le disque dur de l'ordinateur personnel et peuvent faire l'objet d'un nouveau calcul à tout moment. Durant cette phase, un ordre de ré-initialisation est transmis par l'ordinateur personnel à la

5 carte. L'ordinateur calcule alors un couple clé publique PKc - clé secrète PKd, puis calcule une signature de la clé publique PKc à l'aide de la clé secrète PKd. Cette signature est transmise, avec la clé publique PKc, vers la carte. Elle est ensuite vérifiée par la carte, à l'aide de la clé publique PKc. La carte calcule alors, à l'aide d'une clé

10 secrète CKd, une signature de la clé publique CKc. Cette signature est transmise, avec la clé publique CKc, vers l'ordinateur personnel. L'ordinateur vérifie la signature, à l'aide de la clé publique CKc.

La phase de transfert est une phase de chargement d'informations secrètes de la carte dans l'ordinateur personnel. Ces

15 informations permettent à l'ordinateur d'effectuer le décryptage de la forme précompilée et cryptée du programme Prgm. Pour cette phase, l'ordinateur demande à la carte le transfert de la clé secrète de décryptage Kd dont elle dispose dans sa mémoire. La carte crypte cette clé en utilisant la clé PKc, et l'envoie à l'ordinateur. Celui ci

20 décrypte ce message à l'aide de sa clé Kd, et dispose ainsi de la clé Kc. Il lui est alors possible de décrypter le programme Kc(Prgm), pour obtenir un programme Prgm', qui n'est autre que le programme originel Prgm si aucune tentative de fraude n'a eu lieu.

L'ordinateur peut à ce moment décomposer le programme

25 Prgm' en unités élémentaires, et leur appliquer la propriété P, comme dans le premier mode de réalisation. Si le résultat est satisfaisant, il archive ledit programme, par exemple sur son disque dur. Il peut

également calculer une information de vérification (par exemple un checksum ou, mieux, un hashing) et l'archiver dans la mémoire de la carte, à des fins de vérification ultérieures d'intégrité du programme.

REVENDECATIONS

1. Procédé de sécurisation de la transmission d'un message Prgm d'un dispositif émetteur E à un dispositif récepteur R, caractérisé en ce que :

- 5 - le message Prgm est divisé en n unités élémentaires I, n étant un nombre supérieur à 1 ;
 - une propriété logique P est définie de manière que, pour toute unité élémentaire I, la propriété logique P, appliquée à une unité élémentaire I authentique, donne une valeur logique du type
- 10 vrai ;
 - le message Prgm est crypté par des moyens de cryptage du dispositif émetteur E à l'aide d'un algorithme de cryptage comportant une clé Kc de manière à obtenir un résultat crypté Kc(Prgm) ;
- 15 - le résultat crypté Kc(Prgm) est transmis par le dispositif émetteur E au dispositif récepteur R ;
 - le résultat crypté Kc(Prgm) est décrypté par le dispositif récepteur R à l'aide d'un algorithme de décryptage comportant une clé secrète Kd de manière à obtenir un résultat décrypté
- 20 Kd(Kc(Prgm)) ;
 - le résultat décrypté Kd(Kc(Prgm)) est divisé en unités élémentaires I ;
 - la propriété logique P est appliquée aux unités élémentaires I de manière à obtenir, pour chaque unité, une valeur logique du
- 25 type vrai ou du type faux ;
 - le message Prgm est considéré comme authentique et intègre si, pour chaque unité, les valeurs logiques ont une valeur du type

vrai.

2. Procédé selon la revendication précédente, caractérisé en ce que le message Prgm est un programme informatique susceptible d'être exécuté et/ou d'être interprété par le dispositif récepteur R.

5 3. Procédé selon la revendication précédente, caractérisé en ce que les unités élémentaires sont des instructions du programme Prgm.

4. Procédé selon la revendication 2 ou 3, caractérisé en ce que la propriété P, appliquée à une unité élémentaire I, donne une valeur
10 logique de type vrai lorsque l'unité élémentaire I est exécutable et/ou interprétable.

5. Procédé selon l'une des revendications 2, 3 ou 4, caractérisé en ce que la propriété P, appliquée à une unité élémentaire I, donne une valeur logique de type faux lorsque l'unité élémentaire I
15 n'est pas exécutable et/ou interprétable.

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que le dispositif récepteur R est un objet portable à mémoire du type carte à puce.

7. Procédé selon l'une des revendications 1 à 5, caractérisé en ce
20 que le dispositif récepteur R comporte un objet portable à mémoire du type carte à puce.

8. Procédé selon la revendication 6, caractérisé en ce que l'objet portable à mémoire est un module d'identification abonné SIM.

9. Procédé selon l'une des revendications précédentes, caractérisé
25 en ce que le message Prgm est écrit dans un langage interprété de haut niveau.

10. Procédé selon la revendication 9, caractérisé en ce que le

langage de haut niveau est le langage Java.

11. Procédé selon l'une des revendications 9 ou 10, caractérisé en ce que le programme informatique est formé d'un ensemble d'instructions précompilées.

5 12. Procédé selon l'une des revendications précédentes, caractérisé en ce que le message Prgm est crypté en flux continu ou en blocs chaînés.

10 13. Procédé selon l'une des revendications précédentes, caractérisé en ce que le message Prgm est crypté en blocs et en ce que les blocs du message Prgm crypté sont permutés.

14. Procédé selon la revendication 13, caractérisé en ce que un des blocs permutés est un bloc de début ou de fin du message Prgm.

15 15. Procédé selon l'une des revendications 1 à 12, caractérisé en ce que le résultat $Kc(Prgm)$ est décrypté par blocs, chaque bloc crypté étant à l'origine d'un bloc décrypté prenant la place du bloc crypté.

20 16. Procédé selon l'une des revendications précédentes, caractérisé en ce que les algorithmes de cryptage et de décryptage font intervenir un aléa, transmis par le dispositif émetteur E, au dispositif récepteur R.

25 17. Procédé selon l'une des revendications précédentes, caractérisé en ce que le message Prgm est enregistré, après vérification, dans une mémoire non volatile du dispositif récepteur R.

INTERNATIONAL SEARCH REPORT

National Application No

PCT/FR 98/02753

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L9/32 G06F12/14 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	WO 97 05551 A (VERIFONE) 13 February 1997 see abstract see page 4, line 9 - line 20 see page 14, line 23 - page 15, line 17 see page 17, line 18 - page 18, line 5; figure 5 ---	1-3 6,7
X	US 5 155 680 A (WIEDEMER) 13 October 1992 see column 10, line 46 - column 12, line 47 see column 17, line 15 - line 49 ---	1-3,13, 14
A	PATENT ABSTRACTS OF JAPAN vol. 097, no. 011, 28 November 1997 & JP 09 179951 A (DAINIPPON PRINTING CO LTD), 11 July 1997 see abstract --- -/--	1,6,7



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

7 April 1999

Date of mailing of the international search report

13/04/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/FR 98/02753

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category ²	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 537 738 A (SOFTWARE SECURITY) 21 April 1993 see column 4, line 37 - column 5, line 26 -----	1-3
A	MORI R ET AL: "SUPERDISTRIBUTION: THE CONCEPT AND THE ARCHITECTURE" TRANSACTIONS OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS OF JAPAN, vol. E73, no. 7, July 1990, pages 1133-1146, XP002010383 TOKYO (JP) see abstract see page 1138, left-hand column, line 3 - right-hand column, line 19 -----	1-3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 98/02753

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9705551	A	13-02-1997	AU 6547696 A EP 0842471 A	26-02-1997 20-05-1998
US 5155680	A	13-10-1992	US 4796181 A CA 1281418 A EP 0265183 A JP 63191228 A US 5047928 A	03-01-1989 12-03-1991 27-04-1988 08-08-1988 10-09-1991
EP 537738	A	21-04-1993	US 5222133 A CA 2080531 A,C DE 69214080 D DE 69214080 T	22-06-1993 18-04-1993 31-10-1996 27-02-1997

THIS PAGE BLANK (USPTO)

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No

PCT/FR 98/02753

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L9/32 G06F12/14 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	WO 97 05551 A (VERIFONE) 13 février 1997 voir abrégé voir page 4, ligne 9 - ligne 20 voir page 14, ligne 23 - page 15, ligne 17 voir page 17, ligne 18 - page 18, ligne 5; figure 5 ---	1-3 6,7
X	US 5 155 680 A (WIEDEMER) 13 octobre 1992 voir colonne 10, ligne 46 - colonne 12, ligne 47 voir colonne 17, ligne 15 - ligne 49 ---	1-3, 13, 14
A	PATENT ABSTRACTS OF JAPAN vol. 097, no. 011, 28 novembre 1997 & JP 09 179951 A (DAINIPPON PRINTING CO LTD), 11 juillet 1997 voir abrégé ---	1,6,7
-/-		

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

7 avril 1999

Date d'expédition du présent rapport de recherche internationale

13/04/1999

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

internationale No

PCT/FR 98/02753

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités. avec le cas échéant. l'indication des passages pertinents	no. des revendications visées
A	EP 0 537 738 A (SOFTWARE SECURITY) 21 avril 1993 voir colonne 4, ligne 37 - colonne 5, ligne 26 ----	1-3
A	MORI R ET AL: "SUPERDISTRIBUTION: THE CONCEPT AND THE ARCHITECTURE" TRANSACTIONS OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS OF JAPAN, vol. E73, no. 7, juillet 1990, pages 1133-1146, XP002010383 TOKYO (JP) voir abrégé voir page 1138, colonne de gauche, ligne 3 - colonne de droite, ligne 19 -----	1-3

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Internationale No

PCT/FR 98/02753

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9705551 A	13-02-1997	AU 6547696 A EP 0842471 A	26-02-1997 20-05-1998
US 5155680 A	13-10-1992	US 4796181 A CA 1281418 A EP 0265183 A JP 63191228 A US 5047928 A	03-01-1989 12-03-1991 27-04-1988 08-08-1988 10-09-1991
EP 537738 A	21-04-1993	US 5222133 A CA 2080531 A,C DE 69214080 D DE 69214080 T	22-06-1993 18-04-1993 31-10-1996 27-02-1997



1
2
3

1
2
3